GETMOBIT

141983, Московская обл., г. Дубна,
ул. Программистов, дом 4, стр. 2, пом. 137
Тел.: +7(495)796-22-96
Эл. почта: info@getmobit.ru
www.getmobit.ru

GMSS New Generation

Описание решения

Функциональные и технические характеристики

GMSS Factory NG: 3.16.2
GM Core Kit: 2.5.2
GMSS NG Client 1.3
Версия документа: 3.2

ОГЛАВЛЕНИЕ

1. Общие сведения

Настоящий документ описывает решение компании «Гетмобит» GMSS New Generation (далее GMSS NG) для построения платформы унифицированного рабочего пространства в концепции Smart Workspace (далее Система) для сотрудников федеральных органов исполнительной власти, ФГУП, МУП, предприятий ОПК, государственных корпораций, предприятий малого и среднего бизнеса и других. Документ описывает концепцию и архитектуру Системы, а также её основные функционально-технические характеристики, средства интеграции как внутри Системы, так и со смежными информационными системами и сервисами.

Ключевой задачей является построение гибкой и адаптивной коммуникационной среды, обеспечивающей удобство работы конечных пользователей, в том числе в различных контурах информационного обмена, операционную эффективность и экономию на владении. Решение GMSS NG максимально универсально и позволяет учесть отраслевую специфику и технические особенности эксплуатации в широком диапазоне вариантов применения.

Т.к. платформа GMSS NG является эволюционным развитием платформы GM Smart System, настоящий документ описывает всю экосистему продуктов GETMOBIT.

2. Назначение и цели создания Системы на базе платформы GMSS NG

Платформа GMSS NG предназначена для обеспечения доступа к информационным системам заказчика – ресурсам прикладных информационных систем с выполнением всех необходимых требований по обеспечению мер информационной безопасности и требований по защите информации, в том числе, в государственных информационных системах.

Целями выполнения работ по внедрению Системы являются:

1. снижение операционных издержек при эксплуатации рабочих мест сотрудников;
2. повышение уровня защищенности информации, обрабатываемой на автоматизированных рабочих местах сотрудников организации;
3. сохранение инвестиций как в части оконечного пользовательского оборудования (тонкие клиенты Dell, HP и т.д. с сопутствующей периферией), так и в части инфраструктурных сервисов – VDI Citrix, VMWare, Microsoft, службы каталогов MS Active Directory и т.д.;

4. осуществление миграции инфраструктурных сервисов на альтернативные решения российских производителей без существенного вмешательства в бизнес-процессы администрирования рабочих мест пользователей;
5. экономия на затратах, связанных с эксплуатацией и технической поддержкой инфраструктуры;
6. поддержание инфраструктуры рабочих места в актуальном состоянии;
7. снижение рисков потери данных из-за сбоев в работе сотрудников;
8. унификация пользовательской рабочей среды (единообразие ОС, ПО и настроек на рабочих местах сотрудников).

Задачи, решаемые при выполнении работ по внедрению Системы:

1. обеспечение централизованного управления рабочими местами сотрудников организации;
2. централизация управления и контроль доступа к информационным ресурсам и сервисам;
3. обеспечение безопасности информации, циркулирующей в информационных системах организации;
4. доступ сотрудников к инфраструктуре виртуальных рабочих столов;
5. поддержка бесшовной интеграции в существующую инфраструктуру с учетом особенностей архитектуры систем, используемых решений различных вендоров, требований к эксплуатации и пользовательского опыта;
6. организация унифицированных многофункциональных рабочих пространств для сотрудников с учетом корпоративных требований информационной безопасности и особенностей ИТ-инфраструктуры с доступом к аудио и видео связи без создания дополнительной нагрузки на среду VDI при расширении парка пользовательского оборудования универсальными док-станциями GM-Box;
7. обеспечение быстрой реакции системы на сбои в подключении к корпоративной инфраструктуре за счет автоматизированной системы диспетчеризации;
8. упрощение процессов развертывания и настройки рабочих мест сотрудников организации, в том числе географически-распределённых.

3. Функции, реализуемые системой

GMSS NG обеспечивает реализацию следующих функций:

1. предоставление пользователям доступа к сервисам виртуальных рабочих столов (VDI) основных отечественных и зарубежных производителей;

2. предоставление пользователям доступа к веб-сервисам;
3. предоставление пользователям доступа к сервисам VoIP-телефонии с использованием протокола SIP;
4. предоставление пользователям доступа к сервисам видео-конференц-связи с использованием протокола SIP или штатными средствами в виртуальной машине пользователя;
5. предоставление возможности использования различных способов и средств защиты информации, в том числе и криптографических, от различных вендоров;
6. предоставление администраторам системы возможности централизованного управления пользовательским оборудованием, включая загрузку сертификатов, конфигурационных файлов VDI клиентов, создание разовых и повторяющихся заданий для отдельных управляемых устройств и групп управляемых устройств;
7. предоставление администраторам возможности централизованного управления политиками использования USB портов управляемых устройств;
8. предоставление администраторам возможности принудительного прекращения сессий пользователей;
9. предоставление администраторам системы возможности централизованного управления учётными данными и профилями пользователей;
10. предоставление администраторам системы возможности централизованного мониторинга состояния пользовательского оборудования;
11. предоставление администраторам системы возможности централизованного обновления системного программного обеспечения пользовательского оборудования;
12. предоставление администраторам системы возможности централизованного обновления прикладного программного обеспечения пользовательского оборудования;
13. распространение системного и прикладного программного обеспечения через распределённую сеть Точек дистрибуции;
14. предоставление пользователям возможности поочерёдного использования одного экземпляра оборудования разными сотрудниками;
15. предоставление возможности использования устройств сторонних производителей в качестве тонких клиентов в единой инфраструктуре АРМ;
16. обеспечение установки системного ПО Getmobit на устройства сторонних производителей с использованием протокола PXE.

4. Применимость системы на объектах автоматизации

Система GMSS NG может применяться для создания автоматизированных рабочих мест (АРМ) сотрудников федеральных органов исполнительной власти, ФГУП, МУП, предприятий ОПК и других организаций, в т.ч. коммерческих.

Оптимальное использование возможностей Системы достигается на объектах автоматизации, оснащённых (оснащаемых) средами VDI, IP (SIP) телефонией, развитыми веб-сервисами и СКЗИ для организации удалённого доступа к рабочей среде.

Применение универсальной док-станции GM-Box в составе GMSS NG возможно для создания системы информационной безопасности защищенных информационных систем (ГИС, КИИ, ИС ПДн), построенных по архитектуре «клиент-сервер» с применением технологии VDI, с условием переноса всех необходимых механизмов безопасности на устанавливаемые на серверы АИС внешние подсистемы.

В том числе возможно применение GMSS NG:

- на объектах автоматизации с обеспечением доступа к информационным системам, в том числе и защищенным информационным системам, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну;
- на ОКИИ первой категории;
- в ГИС первого класса защищённости;
- в АСУ (ТП) первого класса защищённости;
- в ИСПДн первого уровня защищённости;
- в ИС общего пользования второго класса.

5. GM Smart System New Generation

Единая доверенная цифровая платформа GM Smart System New Generation предназначена для построения унифицированного коммуникационного рабочего пространства с централизованной системой управления конечными устройствами и доступом пользователей к корпоративным информационно-вычислительным ресурсам.

Цифровая платформа GMSS NG состоит из:

- системы централизованного управления и мониторинга GMSS NG FACTORY NG

В состав GMSS NG FACTORY входят следующие компоненты:

- сервер управления (NG FACTORY) с сервисами логирования и мониторинга;
- веб-консоль;
- агент GM Agent[1];
- модуль сервера управления GM Smart System New Generation. Distribution Point.

Платформа GMSS NEW GEN также обеспечивает:

- обратную совместимость с универсальными док-станциями GM-Box со встроенным программным обеспечением GM CORE KIT (устройство клиентского доступа к информационным ресурсам и сервисам компании);
- совместимость с ранее доступными и вновь выпускаемыми SD App-приложениями (Smart Desktop Application), устанавливаемыми на управляемые устройства.

Под клиентскими устройствами в составе платформы GMSS NG понимаются:

- универсальные док-станции GM-Box;
- совместимые устройства – ПК, ноутбуков, тонких клиентов – сторонних производителей, с установленным программным обеспечением GM SS Client NG (устройство клиентского доступа к информационным ресурсам и сервисам компании).

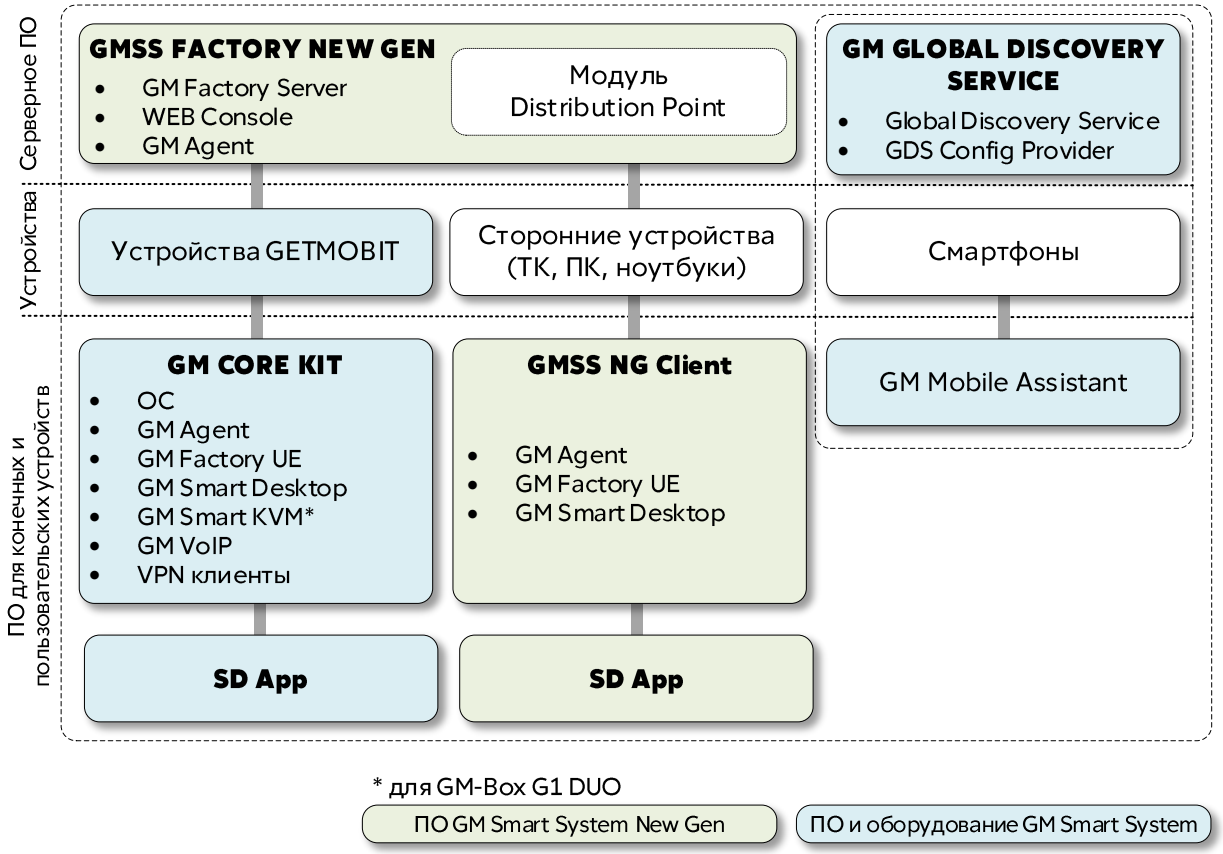
Встроенное программное обеспечение GM CORE KIT и GM SS Client NG обеспечивает корректное функционирование адаптированного стороннего программного обеспечения на клиентских устройствах и выполняет следующие функции:

- обеспечение доступа пользователей к сервисам виртуальных рабочих станций (Virtual Desktop Infrastructure), выполнение роли тонкого клиента;
- обеспечение доступа пользователей к сервисам унифицированных коммуникаций: мультимедиа, VoIP-телефонии, видеосервисам (для устройств GM-Box);
- обеспечение доступа пользователей к веб-сервисам;
- предоставление администраторам возможности централизованного управления устройствами клиентского доступа, учётными данными и профилями пользователей;

[1] Совместимость клиентского ПО с опциональным сервисом Global Discovery Service (GDS) и мобильным приложением GM Mobile Application, выпускаемого для платформы GM SS New Gen, будет реализована в следующих релизах ПО.

– предоставление администраторам возможности централизованного мониторинга состояния устройств клиентского доступа.

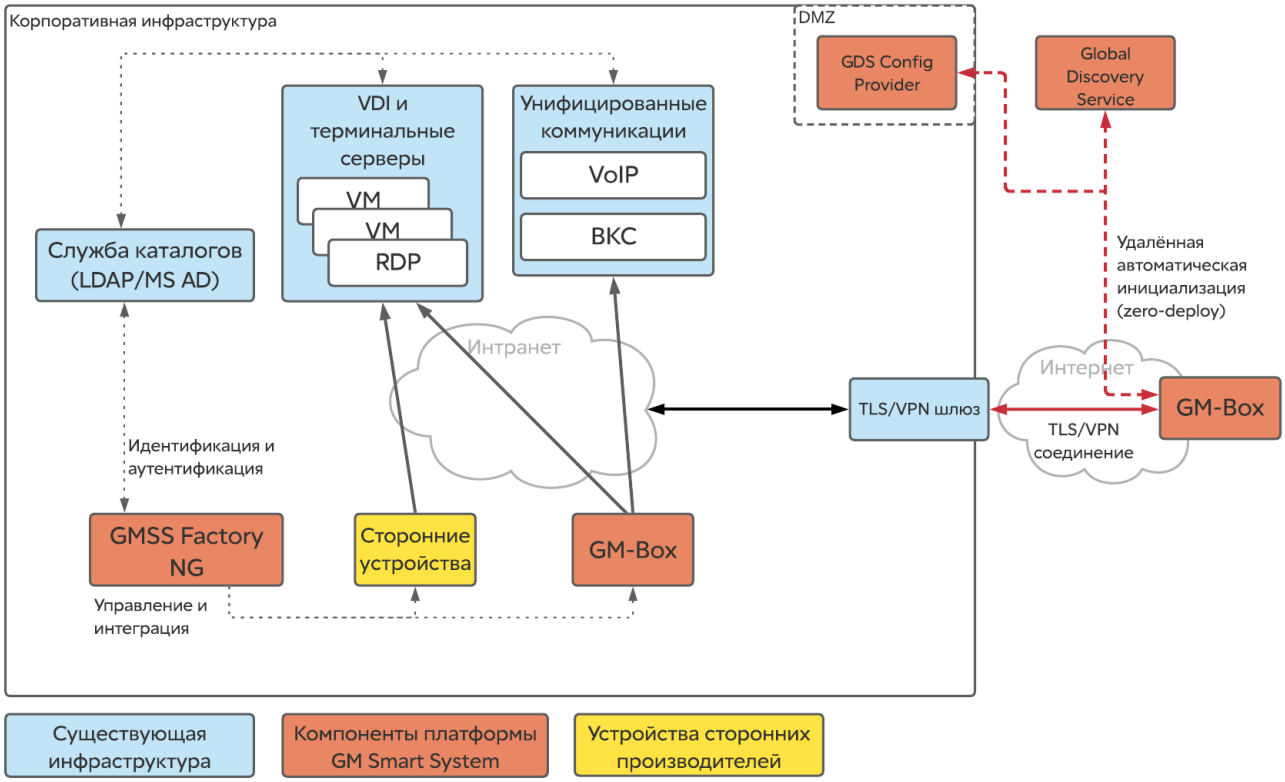
Компоненты единой доверенной рабочей среды приведена на следующей схеме:



Компоненты единой доверенной рабочей среды

5.1. Типовая схема информационной системы

Типовая схема информационной системы представлена на рисунке ниже:



Типовая схема информационной системы

Типовая информационная система включает:

- Подсистему управления инфраструктурой рабочих мест GMSS NG в составе:
  - Сервер управления GMSS NG FACTORY
  - Клиентские устройства – GM-Box и устройства сторонних производителей (с установленным GMSS NG CLIENT
- Подсистему виртуальных рабочих мест в составе:
  - Среда виртуализации
  - Среда VDI
  - Терминальные серверы
- Прикладные подсистемы, включая веб-сервисы и серверы приложений
- Подсистему коммуникаций:
  - Сетевые сервисы
  - VoIP
  - ВКС и UC

- Подсистему информационной безопасности:
  - Средства межсетевого экранирования, СОВ и СКЗИ
  - Антивирусную защиту
  - Средства контроля и мониторинга
  - Средства идентификации, аутентификации и управления доступом

5.2. Функциональные и технические характеристики

1.1.1. Универсальная Док-Станция GM-Box G1[2]

Универсальная док-станция GM-Box G1 выпускается в двух модификациях: GM-Box Base и GM-Box DUO.

Модификация GM-Box Base основана на базе одного вычислительного модуля и предназначена для работы в одноконтурной сетевой инфраструктуре.

Модификация GM-Box DUO предназначена для работы в двухконтурной сетевой инфраструктуре с использованием одного физического устройства за счёт объединения в рамках одного устройства возможностей двух независимых вычислительных модулей и KVM-переключателя.

Устройства модификации BASE обладают следующими характеристиками:

- архитектура процессора – x86;
- 4 физических вычислительных ядра;
- 4 потока;
- базовая частота – 1,1 ГГц, до 2,2 ГГц;
- оперативная память – 4 Гб;
- энергонезависимая память – 16 Гб;
- 1 разъём HDMI (версия 1.4b);
- 1 разъём DisplayPort (версия 1.2);
- встроенный цветной монитор с разрешением 1280 x 720 пикселей;
- встроенная цветная видеокамера с разрешением 1280 x 720 пикселей.
- наличие телефонной трубки со встроенным микрофоном и динамиком;
- разъем для подключения телефонной трубки;
- количество встроенных динамиков – 2, каждый мощностью не менее 2 Вт;
- количество встроенных микрофонов – 2;
- 1 аудиоразъём 3.5 мм с поддержкой микрофонного входа;

[2] Входит в состав GM Smart System и совместима с GMSS NG

- 1 разъём Ethernet 10/100/1000 Мбит/с;
- WiFi (802.11n/ac) модуль для отдельных исполнений;
- NFC, Qi и RFI модули для отдельных исполнений;
- АПМДЗ соболь для отдельных исполнений;
- 5 разъёмов USB 2.0;
- 3 разъёма USB 3.0;
- поддержка внешних переходников с USB на COM/LPT (список совместимых устройств предоставляется по запросу);
- поддержка пассивных переходников с HDMI на DVI (список совместимых устройств предоставляется по запросу);
- поддержка активных переходников с HDMI/DP на VGA (список совместимых устройств предоставляется по запросу).

Устройства модификации DUO обладают следующими характеристиками:

- архитектура процессора – x86 на основном и дополнительном ВМ;
- 4 физических вычислительных ядра для основного ВМ, 2 физических ядра для дополнительного ВМ;
- базовая частота –1,1 ГГц, до 2,2 ГГц;
- оперативная память основного ВМ – 4 ГБ;
- оперативная память дополнительного ВМ – 4 ГБ;
- энергонезависимая память основного ВМ – 32 ГБ;
- энергонезависимая память дополнительного ВМ – 32 ГБ;
- встроенный ПАК GM SMART KVM – программно-управляемый коммутатор USB и HDMI интерфейсов;
- 1 разъём HDMI (версия 1.4b), коммутируемый между вычислительными модулями через встроенный KVM;
- 1 разъём Ethernet 10/100/1000 Мбит/с на каждом вычислительном модуле;
- Интерфейсы и устройства основного ВМ:
    - 1 разъём DisplayPort;
    - встроенный цветной монитор с разрешением 1280 x 720 пикселей;
    - встроенная цветная видеокамера с разрешением 1280 x 720 пикселей;
    - наличие телефонной трубки со встроенным микрофоном и динамиком;
    - разъем для подключения телефонной трубки;
    - количество встроенных динамиков – 2, каждый мощностью не менее 2 Вт;
    - количество встроенных микрофонов – 2;
    - 1 аудиоразъём 3.5 мм с поддержкой микрофонного входа;

  - WiFi (802.11n/ac) модуль для отдельных исполнений;
  - NFC, Qi и RFI модули для отдельных исполнений;
- АПМДЗ соболь для отдельных исполнений (возможна установка на основном и дополнительном ВМ);
- 2 разъема USB 2.0, 2 разъема USB 3.0 (основной ВМ);
- 2 разъема USB 3.0 (дополнительный ВМ);
- 2 разъема USB 2.0, подключенных через встроенный KVM и коммутируемых между вычислительными модулями;
- поддержка внешних переходников с USB на COM/LPT (список совместимых устройств предоставляется по запросу);
- поддержка пассивных переходников с HDMI на DVI (список совместимых устройств предоставляется по запросу);
- поддержка активных переходников с HDMI/DP на VGA (список совместимых устройств предоставляется по запросу).

В GM-Box DUO реализовано физическое разграничение открытого и закрытого контура корпоративной сети посредством раздельного подключения независимых вычислительных модулей к сетевым сегментам и с возможностью переключения между ними при помощи встроенного аппаратного KVM-переключателя (Keyboard-Video-Mouse).

К GM-Box Base и GM-Box DUO могут быть подключены локальные совместимые USB принтеры. Подключение локального принтера к GM-Box DUO выполняется посредством USB-порта, подключённого к соответствующей плате открытого или закрытого контура устройства. Для работы с локальным принтером необходимо подключить его к USB-порту платы GM-Box DUO соответствующего сетевого контура.

1.1.2. GMSS NG FACTORY

GMSS NG FACTORY – серверное программное обеспечение для централизованного управления устройствами, обновления, профилирования, мониторинга, журналирования и масштабирования. GMSS NG FACTORY позволяет строить масштабируемые и отказоустойчивые решения без ограничения горизонтального масштабирования.

GMSS NG FACTORY поддерживает:

- возможность интеграции со службами каталогов совместимыми с LDAP такими, как FreeIPA, ALD Pro, MS Active Directory;
- возможность централизованного управления учётными данными и профилями пользователей;

- возможность создания и управления шаблонами настроек профилей пользователей с целью автоматизации и реализации бизнес-сценариев использования системы;
- возможность централизованного управления клиентскими устройствами;
- автоматизацию первичной настройки управляемых устройств и упрощение типовых задач администрирования благодаря автоматической детекции устройств, требующих проведение первичной настройки и формирования сценариев команд для настройки;
- возможность централизованного мониторинга состояния клиентских устройств;
- возможность управления режимами работы клиентских устройств с учётом их возможностей и профиля пользователя (монорежим, режим «витрины», веб-режим, гостевой режим);
- возможность централизованного обновления системного программного обеспечения клиентских устройств;
- возможность загрузки сертификатов на клиентские устройства;
- возможность установки и настройки плагинов в формате Smart Desktop приложений (SDApp) на клиентские устройства;
- возможность централизованного журналирования событий с клиентских устройств;
- горизонтальное масштабирование, построение решений высокой доступности с балансировкой нагрузки;
- возможность интеграции с корпоративными сервисами.

1.1.3. GMSS NG. Distribution Point

GM Smart System New Generation. Distribution Point – это программный модуль, реализующий функционал точек дистрибуции обновлений, прикладного программного обеспечения в формате SDApp и файлов для системы централизованного управления и мониторинга GMSS NG FACTORY (GM Smart System New Generation Factory). Точки Дистрибуции (Distribution Point) позволяют географически-распределённым компаниям минимальными усилиями поддерживать инфраструктуру рабочих мест в актуальном состоянии и обеспечивают гарантированную доставку обновлений и приложений, обеспечивают снижение нагрузки на магистральные каналы связи.

Модуль Distribution Point обеспечивает:

- хранение, доставку и централизованный контроль обновлений;
- снижение нагрузки на магистральные каналы связи при обновлениях ПО – файлы распространяются в прикреплённой к точке дистрибуции подсети;

- управление скоростью отдачи файлов;
- создание георасределённой инфраструктуры репозиториев ПО – точек дистрибуции – в соответствии с организационной структурой компании;
- поддержание состояния системы в актуальном состоянии во всей организации – своевременное гарантированное обновление встроенного ПО и SDApp;
- функционал встроенного DHCP Proxy
- функционал встроенного PXE сервера.

1.1.4. Программное обеспечение клиентских устройств GM-Box

Программное обеспечение GM CORE KIT предустановлено (с возможностью обновления до новых версий) на клиентские устройства GM-Box. Встроенное ПО GM CORE KIT устанавливается на устройства GM-Box модификаций BASE и DUO.

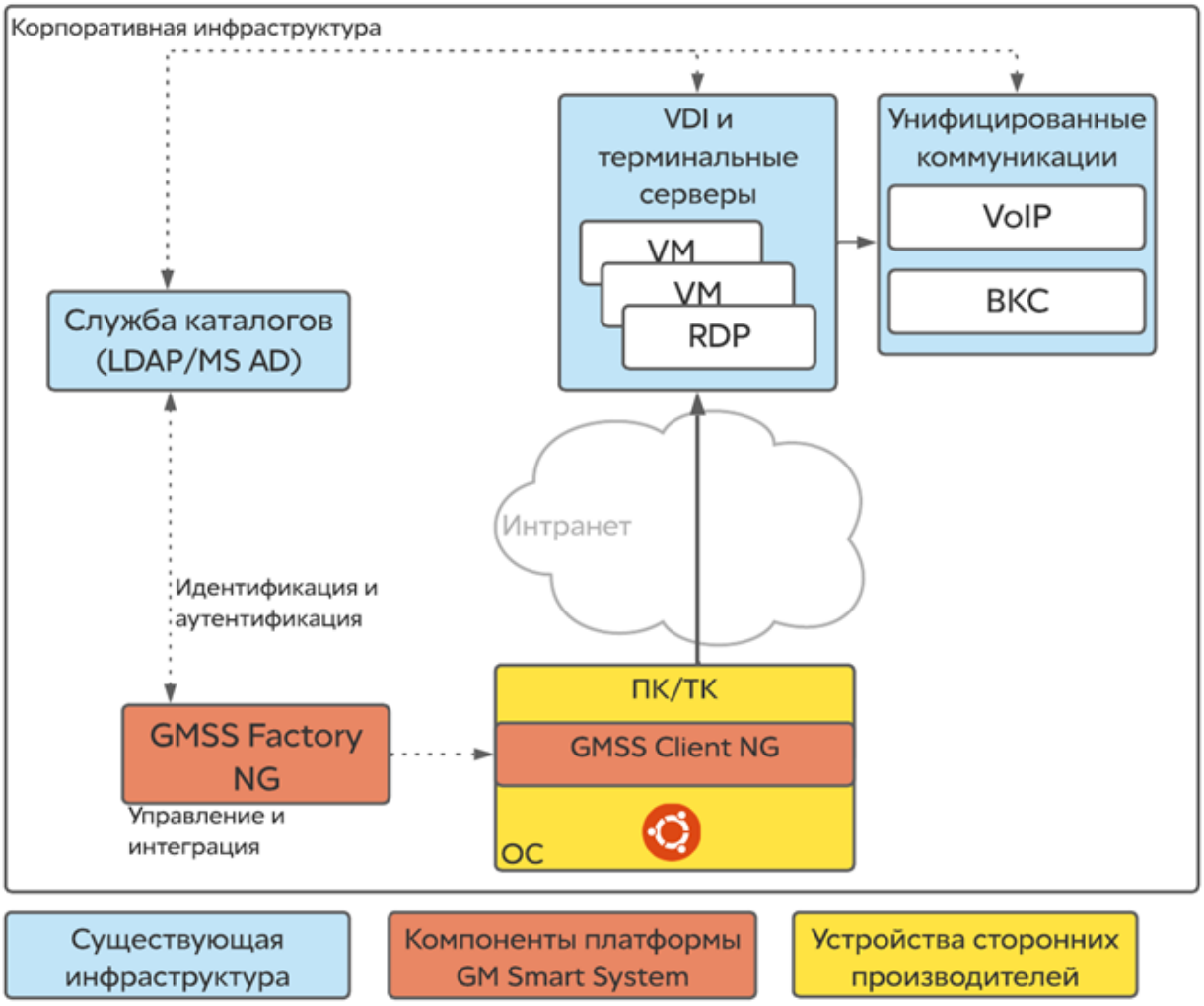
GM CORE KIT обеспечивает:

- возможность поочерёдного использования одного устройства разными сотрудниками в любом из поддерживаемых режимов (с учётом настроек профиля пользователя):
  - веб-режим;
  - терминальный или VDI режим;
  - режим «Витрины»;
  - гостевой режим.
- возможность использования коммуникационных VVoIP (Video & Voice over IP) сервисов на базе протокола SIP;
- взаимодействие с мобильным приложением GM Mobile Assistant;
- работу в сетевой среде Ethernet;
- работу в сети Wi-Fi;
- работу в сети 4G/LTE;
- возможность вывода изображения на два монитора;
- поддержку протокола LDAP, включая Microsoft Active Directory;
- возможность запуска установленных SDApp приложений;
- поддержку собственных средств централизованного управления и мониторинга состояния устройств, входит в компоненту сервера управления;
- поддержку собственных средств централизованного мониторинга событий информационной безопасности, входит в компоненту сервера управления;

- поддержку собственных локальных средств диагностики;
- поддержку автоматизированной первичной инициализации при удалённом доступе.

1.1.5. GMSS NG Client - программное обеспечение клиентских устройств на базе устройств сторонних производителей

Для включения устройств сторонних производителей в контур управления платформы GMSS NG, на них должно быть установлено программное обеспечение GMSS NG Client[3]. Типовая схема применения устройств сторонних производителей в экосистеме GMSS NG приведена ниже.



Типовая схема экосистемы GMSS NG с устройствами сторонних производителей

Программное обеспечение GMSS NG Client обеспечивает следующий функционал:

[3] Требования к установке GMSS NG Client постоянно актуализируются и доступны по запросу.

- единый профиль пользователя для всей экосистемы GMSS NG, независимо от устройства;
- единый механизм администрирования и эксплуатации устройств в экосистеме GMSS NG;
- возможность поочерёдного использования одного устройства разными сотрудниками в любом из поддерживаемых режимов (с учётом настроек профиля пользователя):
  - веб-режим;
  - терминальный или VDI режим;
  - режим «Витрины»;
  - гостевой режим.
- работу в сетевой среде Ethernet;
- работу в сети Wi-Fi;
- возможность вывода изображения на два монитора;
- поддержку протокола LDAP, включая FreeIPA, ALD Pro, Microsoft Active Directory;
- возможность запуска установленных SDApp приложений;
- поддержку собственных средств централизованного управления и мониторинга состояния устройств, входит в компоненту сервера управления;
- поддержку собственных средств централизованного мониторинга событий информационной безопасности, входит в компоненту сервера управления;
- поддержку собственных локальных средств диагностики;
- поддержку автоматизированной первичной инициализации при удалённом доступе.

1.1.6. Установка GMSS NG Client на устройства сторонних производителей

Установка GMSS NG CLIENT на устройства сторонних производителей возможна как в ручном, так и автоматизированном режиме при выполнении рекомендаций к таким устройствам, обозначенным в документе «Требования к инфраструктуре».

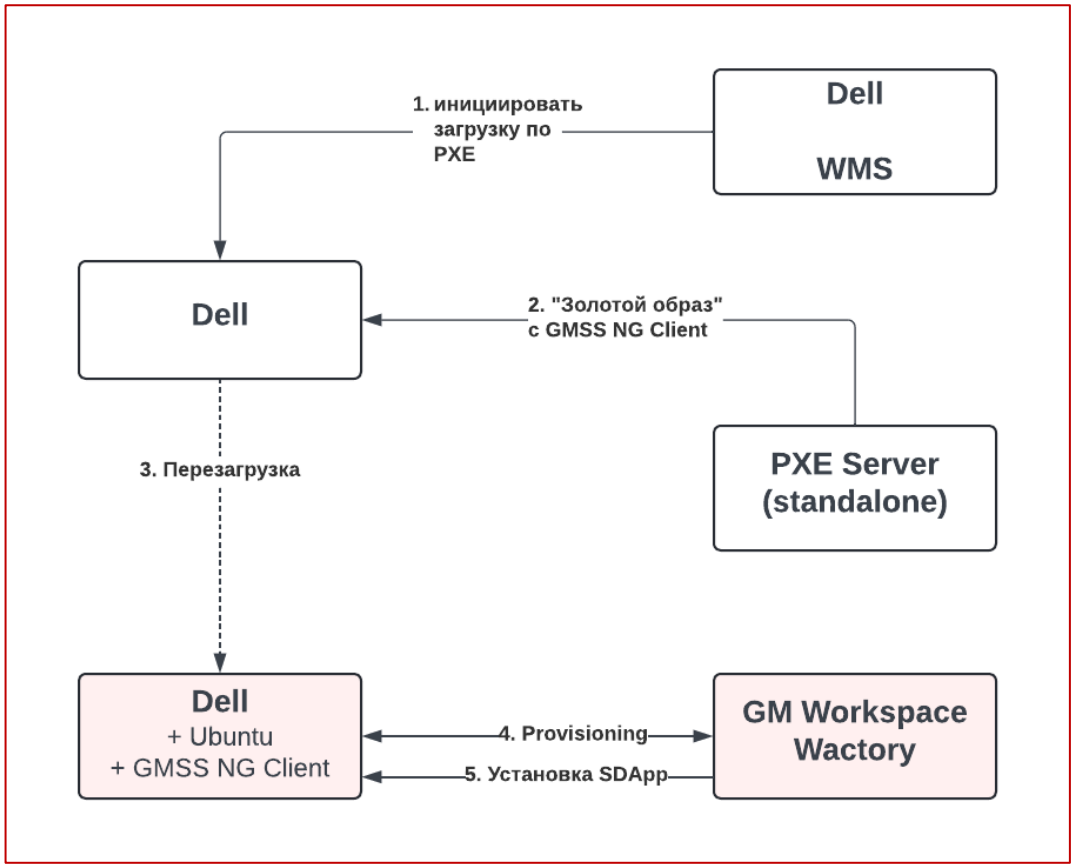
Для установки GMSS NG CLIENT в ручном режиме, необходимо:

1. установить поддерживаемую операционную систему на конвертируемое устройство (например, Ubuntu 20.04 LTS Server)
2. установить дистрибутив GMSS NG Client на конвертируемое устройство.

Для установки GMSS NG CLIENT в автоматизированном режиме необходимо:

1. подготовить установочный образ для установки по PXE или с USB Flash носителя
2. в BIOS устройства выбрать режим загрузки по сети (для варианта PXE) или с внешнего носителя (установка с USB Flash).

В случае, когда производится массовая конвертация устройств с существующей системой управления, поддерживающей управление опциями BIOS (например, Dell Wyse Management Suite или HP Device Manager), возможна массовая конвертация таких устройств. В качестве PXE сервера используется серверный модуль GMSS NG Distribution Point. Необходимые для конвертации файлы загружаются администратором через единую консоль сервера управления GMSS NG Factiry. Конвертация устройств на примере тонких клиентов Dell под управлением Dell Wyse Management Suite представлена на рисунке ниже.



1.1.7. Поддержка режимов терминального доступа

Встроенное ПО поддерживает следующие VDI клиенты и протоколы:

- VDI SPACE, протоколы SPICE, RDP;
- VDI BASIS, протоколы SPICE, RDP, RX[4];
- VDI VeiL, протоколы SPICE, RDP;
- VDI Термидеск, протоколы SPICE, RDP;
- Citrix, протоколы: HDX, ICA;
- Microsoft, протоколы: RDP, RemoteFX;
- VMware, протоколы PCoIP, Blast Extreme;
- Huawei, протокол: HDP;
- Тионикс, Скала-Р, протокол RDP[5];
- Горизонт-ВС, протоколы: Spice, VNC.

Примечание: совместимые версии VDI приведены в Требованиях к инфраструктуре, а также актуализируются в Информационных бюллетенях о новых выпусках ПО (release notes).

Примечание: возможность встраивания дополнительных клиентов VDI и протоколов уточняется по запросу.

1.1.8. Реализация способов входа в систему

Встроенное ПО реализует различные способы идентификации/аутентификации/авторизации пользователя, а именно:

- идентификацию/аутентификацию/авторизацию с использованием логина и пароля;
- идентификацию с использованием USB-токена[6];
- идентификацию с использованием бесконтактной карты;
- идентификацию с использованием смарт-карт, через внешние USB-ридеры смарт-карт;
- идентификацию/аутентификацию с использованием смартфона (Phone-as-a-token) на базе Android или iOS. Для идентификации/аутентификации необходимо загрузить из AppStore или Google Play на смартфон приложение GM MOBILE ASSISTANT;

[4] Поддержка запланирована для будущих релизов SDApp BASIS.

[5] Устаревшие среды VDI, поддержка и развитие в новых версиях ПО не предусмотрено.

[6] Идентификация и аутентификация способами отличными от логина и пароля для GMSS NG Client будет реализована в следующих версиях ПО

– обеспечивает возможность сквозной аутентификации пользователя в домене FreeIPA/ALDPro/Microsoft Active Directory/LDAP.

1.1.9. Поддержка автоматических телефонных станций[7]

Встроенное ПО работает со следующими АТС:

– АТС, совместимые с SIP протоколом (RFC 3261);
– Communigate Pro;
– Eltex;
– Протей;
– Cisco UCM;
– Avaya
– Asterisk;
– Elastix;
– Huawei;
– Freeswitch.

1.1.10. Реализация функций унифицированных коммуникаций[8]

Встроенное ПО обеспечивает следующие возможности унифицированных коммуникаций:

– поддерживает протокол SIP для осуществления телефонных вызовов (голосовых вызовов);
– поддержка аудиоконференций;
– поддерживает видеокодек H.264 для выполнения видеозвонков;
– обеспечивает возможность постановки звонка на удержание;
– обеспечивает возможность переводов звонков на других абонентов;
– обеспечивает возможность повторного набора номера;
– обеспечивает возможность хранения истории звонков;
– обеспечивает возможность уведомлений о пропущенных вызовах;
– поддерживает работу с сервисами голосовой почты;
– синхронизация контактов адресной книги с корпоративным LDAP/AD каталогом.

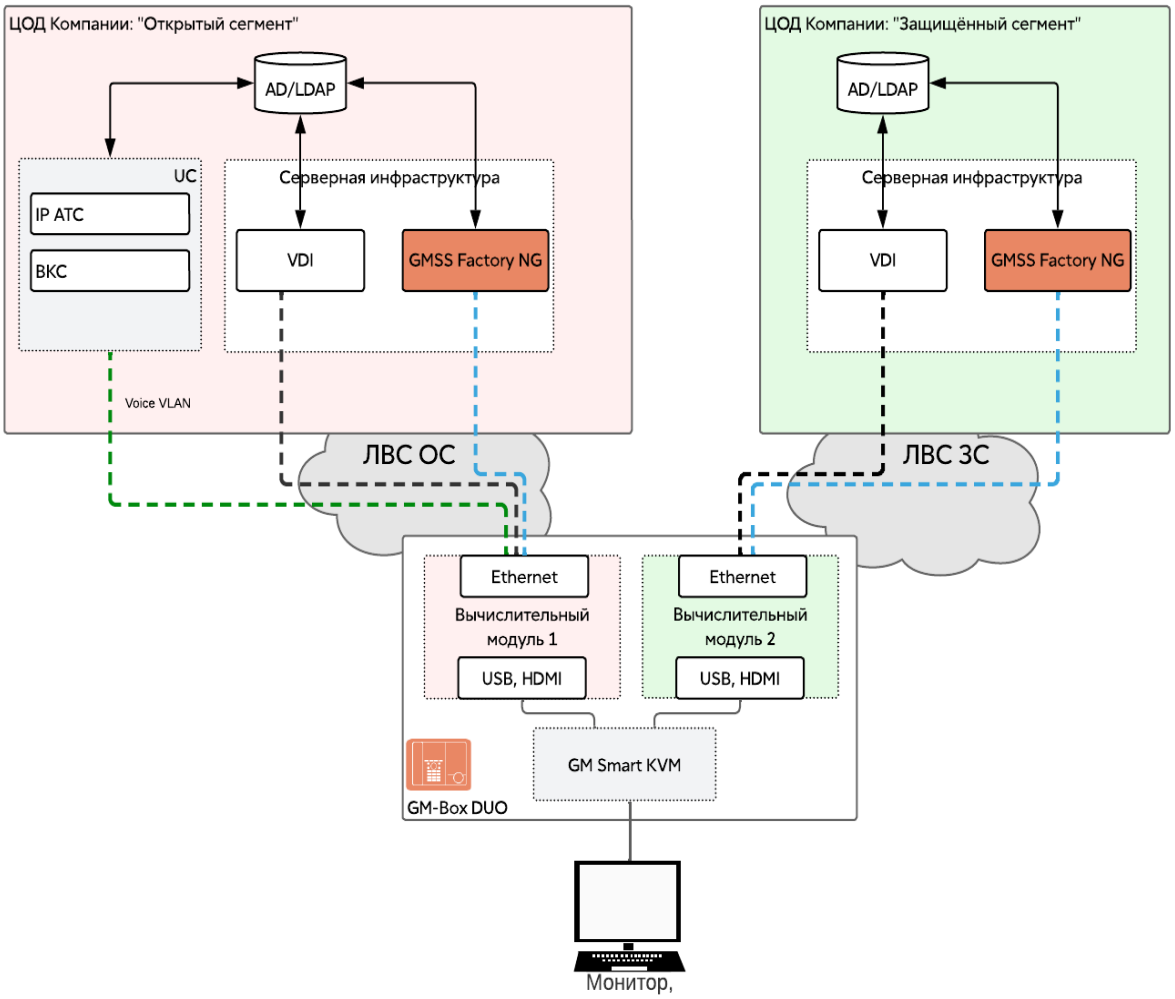
[7] Для устройств GM-Box
[8] Для устройств GM-Box

1.1.11. Обеспечение работы в двухконтурной сети[9]

Встроенное ПО в модификации GM-Box DUO дополнительно обеспечивает следующую функциональность:

- поддерживает работу в двух независимых контурах сети;
- поддерживает встроенный аппаратный KVM-переключатель для переключения монитора, аудиовыхода и USB-устройств между контурами.

Типовая схема применения GM-Box DUO для работы в двухконтурной сети приведена ниже:



Типовая схема применения GM-Box DUO в двухконтурной сети

[9] Для устройств GM-Box DUO

1.1.12. Обеспечение функций информационной безопасности

При подключении к инфраструктуре организации решение «Гетмобит» в полной мере использует существующие информационные системы организации: виртуальную инфраструктуру рабочих мест (VDI), IP-телефонию (VoIP), системы видео-конференц-связи (ВКС) по протоколу SIP, средства криптографической защиты информации. Система допускается к использованию в значимых объектах критической информационной инфраструктуры до 1 категории значимости, удовлетворяет приведенным в соответствующих приказах ФСТЭК России и ФСБ России требованиям, не требует проведения дополнительных сертификационных испытаний или дополнительных доработок.[10]

GMSS NG обеспечивает следующую функциональность:

- для клиентских устройств GM Box:
  - невозможность доступа в BIOS на устройствах (вход в BIOS устройства GM-Box заблокирован);
  - невозможность внесения изменений пользователем в настройки системы;
  - невозможность загрузки с внешних устройств, выбора последовательности и режимов загрузки;
  - невозможность перезаписать встроенное ПО локально;
  - невозможность установки пользователем стороннего ПО;
- Для всех управляемых в экосистеме GM SS NEW GEN устройств[11]:
  - возможность централизованного обновления, встроенного ПО;
  - возможность построение TLS туннеля с применением алгоритмов ГОСТ для передачи трафика от устройства GM-Box до информационной инфраструктуры;
  - возможность построения VPN туннелей с применением предустановленных клиентов ViPNET, OpenVPN[12];
  - возможность подключения к серверу управления по протоколу HTTPS (TLS);

[10] По запросу, может быть предоставлена актуальная аналитическая записка по вопросам применимости GM SS в информационных системах в зависимости от предъявляемых требований информационной безопасности.

[11] Для устройств сторонних производителей возможно использование дополнительных наложенных средств с целью достижения отдельных возможностей

[12] Для устройств GM-Box. Поддержка для GMSS NG Client запланирована в будущих релизах.

- возможность соединения с VDI-брокером по протоколу HTTPS (при наличии реализации функционала брокером и VDI клиентом);
- возможность передачи голосового трафика в отдельный VLAN (LLDP, CDP);
- управление профилями пользователя через централизованную систему управления;
- невозможность изменения пользователем настроек своего профиля и произвольного выбора режима работы;
- возможность управления доступностью USB-портов для пользователя на устройстве GM-Box через централизованную систему управления;
- возможность блокирования локальных изменений сетевых настроек на устройстве через централизованную систему управления;
- возможность создания дополнительных ролей и гибкой настройки политик доступа для администрирования системы управления;
- синхронизация пользователей с корпоративной службой каталогов LDAP/MS AD;
- синхронизация разных ролей пользователей (администраторов) с группами и учётными записями в LDAP/MS AD;
- сервер управления не хранит пароли пользователей при синхронизации с корпоративным LDAP/MS AD;
- возможность поддержки доменной аутентификации для пользователей клиентских устройств;
- возможность поддержки доменной аутентификации для пользователей (администраторов) сервера управления;
- возможность получения информации о статусе конкретного вычислительного модуля устройства GM-Box (GM-Box BASE – 1 вычислительный модуль, GM-Box DUO – 2 вычислительный модуль);
- невозможность произвольного удаленного доступа к устройству GM-Box (протоколы удалённого доступа по умолчанию отключены и могут быть временно запущены только по команде администратора системы управления);
- возможность просмотра на сервере управления журнала событий с устройства;
- возможность экспорта логов в сторонние системы по протоколу;
- возможность управления перезагрузкой, выключением устройств, принудительным завершением сессии пользователя;

- возможность установки и использования АПМДЗ (доверенная загрузка от запуска микропрограммы BIOS до начала загрузки операционной системы на плате вычислительного модуля).

1.1.13. Ролевая модель

GM SS Factory NG позволяет реализовать гибкую ролевую модель. Роли используются для ограничения прав доступа пользователей к разделам веб-консоли. Например, конкретной роли можно разрешить просмотр списка устройств, но отключить возможность отправлять задания на управляемые устройства.

Создавать, редактировать или удалять роли может администратор с соответствующими правами.

По умолчанию доступны следующие системные роли:

- USER – учётная запись с ограниченными правами, используется для аутентификации пользователей на управляемых устройствах;
- ADMIN – учётная запись, которая используется для администрирования СУ, позволяет управлять профилями пользователей и устройств;
- SECURITY – учётная запись, позволяет управлять профилями сотрудников отдела безопасности и создавать задания с командами, разрешёнными SUPER_ADMIN;
- SUPER_ADMIN – учётная запись с максимальными правами, имеет доступ ко всей функциональности СУ, включая возможность создания и редактирования команд.

1.1.14. Языковая поддержка

GMSS NG обеспечивает следующую языковую поддержку:

- в качестве основного языка взаимодействия с пользователями используется русский язык. Графический интерфейс GMSS NG реализован на русском языке;
- в GMSS NG предусмотрена возможность взаимодействия с пользователем на английском языке.

1.2. Требования к инфраструктуре

Для полноценного функционирования GMSS NG должны быть выполнены требования к инфраструктуре. Требования к инфраструктуре описаны в отдельном документе: «Требования к инфраструктуре».